North Carolina Statewide Technical Architecture

Collaboration Domain

Office of the State Chief Information Officer
Enterprise Technology Strategies
PO Box 17209
Raleigh, North Carolina 27699-7209
http://www.ncsta.gov
ets@ncmail.net

Table of Contents

1. Principles:

1.1. Effective uses of collaboration technologies connect people, processes, and information to meet business requirements.

Rationale:

- Content Management, communications, and workflow are key infrastructure components necessary to facilitate collaboration.
- Effective collaboration is enabled by supplying trained personnel with appropriate technologies supported by efficient processes.
- Collaboration allows teams to share and synchronize information and resources. Collaboration technologies enhance this capability by removing boundaries of time, organization, and place.
- Signs of effective collaboration include the following:
  - Reduction of duplication or redundant efforts.
  - Increased awareness of the activities, deliverables, and capabilities of team members.
  - Effective and coordination revision and rework of team deliverables.

1.2. Collaboration technologies link people, processes, and information within and across organization boundaries and are most effective when implemented using an enterprise approach Text

Rationale:

- By its nature, collaboration links people, processes, and information within and across organization boundaries. This linkage can occur through formal or ad hoc establishment of working relationships to achieve a business objective.
- Creation of collaboration systems based on broader, enterprise considerations is more likely to produce adaptive business solutions.
- Though point solutions for localized workgroup collaboration may provide improved user productivity, their true benefit can best be realized through wide-spread integration into processes, workflow, and applications.
- Effective use of collaborative technologies provides a high degree of transparency by hiding the complexity of any underlying technologies in favor of accomplishing the business objective.

1.3. Collaborative technologies are supported and complemented by enterprise-class services.

Rationale:

- Collaboration technologies enable organizations to create, share, and leverage knowledge within and across organizational boundaries. Enterprise collaboration requires universal access to a robust set of integrated infrastructure services.

Collaboration is best supported by integrating standards-based, enterprise class services such as the following:

- Directories
- Identity management
- Access control
- Content and document management
- Resource identification, discovery, and change management
- Synchronous and asynchronous communications
- Portal integration

1.4. Collaborative systems provide the most value when they are designed, acquired, developed, and enhanced to share and integrate data and processes across the enterprise.

Rationale:

- Collaborative technologies and their use in the workplace are constantly evolving. Adapting to these changes can best be achieved by deploying systems based on industry standards.
- Collaborative technologies that can be easily adapted to changes in the environment, without requiring a high degree of custom or proprietary code, preserves and leverages investments in personnel training, hardware, and software, and supports integration with future applications and business processes.
- Planning for adaptability will help accommodate future changes in collaborative technologies.

1.5. Implementation of collaboration technologies are successful when using industry-proven, mainstream technologies that adhere to industry standards and open architecture.

Rationale:

- Selecting application components that adhere to industry standards allows for flexibility, adaptability, and interoperability with other business solutions in the state.
- Collaborative technologies must support multiple server, workstation, and application platforms.
- Use of widely-adopted industry standard approaches to collaboration removes dependencies on the underlying platforms, applications, and tools.
- Choosing proprietary and/or closed systems may result in higher costs to migrate to new technologies.
- Proprietary, closed systems introduce unnecessary integration complexity, maintenance costs, and can lead to vendor lock-in.

1.6. Collaboration systems use standard Application Programming Interfaces (APIs) in order to enable integration.

Rationale:

- Use of standard APIs enables collaborative technologies to be used by other state owned and operated business solutions.
- Collaboration systems that use standard APIs avoid the use of proprietary programming languages and coding practices and mitigate the risk of vendor lock-in.
- Standard API's reduce complexity and increase reusability.

1.7. Collaborative technologies protect the public interest and privacy of the State's citizens and employees when deployed consistently with regulatory and ethical obligations.

Rationale:

- Shared work environments and rich collaboration capabilities do not obviate the need for meeting regulatory and ethical requirements and acceptable use policies.
- Information created, exchanged, and stored via collaborative technologies must be classified and managed consistent with applicable statutes, policies, and regulations pertaining to availability, retention, integrity, and security.

2. Technical Topic: Content Management

2.1. Practices:

2.1.1. Follow guidelines for imaging systems established by the North Carolina Department of Cultural Resources (NC DCR), Office of Archives and History.

Rationale:

- Imaging provides the ability to capture, store, retrieve, and share enormous amounts of structured and unstructured information.
- The NC DCR has prepared a comprehensive guide to using digital imaging systems. This document provides legal and historical background as well as guidelines for planning, technology evaluation and selection, and implementation of imaging systems.
- For more information refer to http://www.ah.dcr.state.nc.us/records/e_records/#guide

2.1.2. Select appropriate storage media for short and long term retention of documents, images, and electronic content.

Rationale:

- Electronic documents, typically created with office automation suites, are initially stored on industry standard magnetic media that is desktop, server, and/or network based.
- Images of scanned documents might also be stored on standard network attached magnetic media. Magnetic storage systems typically provide the most performance in the speed of retrieval, and magnetic disk is becoming more cost competitive with optical disk storage.
- Very large document collections (usually image applications) typically require optical storage subsystems. Optical storage, in the form of Write Once Read Many (WORM)

disk media, should meet most business requirements for the permanent storage of unalterable documents. It is also removable and can easily be stored off-site for safer archiving.

- These types of systems generally involve special software that is used to manage the storage and movement of documents from optical to magnetic when documents are requested by users. Optical disks may be mounted in single standalone drive units or they may be loaded into various sizes of "juke boxes." Software handles the retrieval and loading of specific disks in response to user requests.

2.1.3. Implement content management solutions that provide robust configuration management and access control capabilities that can be integrated with enterprise identity management services.

Rationale:

- Fine grained access control should be applied to protect the intellectual property of works created by and for the state.
- Configuration management provides a means to track changes to works in progress via check-in/out, comment tracking, and versioning.
- Augmenting the content development process with configuration management can most effectively be achieved by integration with enterprise level identity management in lieu of maintaining application specific user databases.

2.1.4. Develop content indexes in accordance with conventions established by the North Carolina Department of Cultural Resources (NC DCR), Office of Archives and History.

Rationale:

- Content developed in the course of performing the state's business functions (whether electronic or manual) may be subject to provisions of the Public Records Law. The North Carolina Department of Cultural Resources (NC DCR) is responsible for administering and enforcing the archival of public records. In order for this archival process to be effective, standards for indexing of structured and unstructured data must be followed.
- Specific guidelines for retention and indexing of government records can be found at http://www.ah.dcr.state.nc.us/

2.2. Standards

2.2.1. The standard for collaborative authoring of web based content is Web Distributed Authoring and Distribution standard (WebDAV).

Rationale:

- WebDAV provides a standard infrastructure for asynchronous collaborative authoring across the Internet. It provides a standard interface between a range of authoring tools and web-based content. An interface and extension to Hypertext Transport Protocol (HTTP), WebDAV supports version management, document locking, and management of metadata such as author and the last date the content was modified.
- WebDAV effectively supports universal collaboration over the Internet.

- Information regarding WebDAV can be found at http://www.webdav.org/

2.2.2. Conform to the North Carolina Public Records Law.

Rationale:

- System design efforts, policy, and procedures for the processing, routing, retention, and disposition of data and documents must be accomplished with respect to public law.
- Content developed and maintained using collaborative technologies (I.e., document management, email, real-time messaging, teamware, etc) are considered public records and must be managed in accordance with the NC Public Records Law.
- For more information regarding the retention and destruction of any electronic records, refer to http://www.ah.dcr.state.nc.us/e-records/default.htm or contact the State Records Center staff at (919) 733-3540.

2.2.3. Implement document management systems and components that conform to the Document Management Alliance specifications.

Rationale:

- There are numerous issues related to interoperability among document management applications, services, and repositories. Standards are needed to manage the increased life expectancy and complexity of re-usable electronic documents and content.
- The Document Management Alliance (DMA) is an Association for Information and Image Management (AIIM) task force consisting of over 60 vendor companies that is working to define interoperability specification to meet requirements for enterprise document management systems.
- The DMA specification defines software component interfaces that enable uniform search and access to documents stored in multi-vendor document management systems.
- The Open Document Management API (ODMA) specifies a set of interfaces that applications can use to initiate actions within a document management system.
- For more information about AIIM standards programs, refer to http://www.aiim.org/standards.asp?ID=24488.

2.2.4. The standard for imaging systems include TWAIN for document imaging and TIFF for storage.

Rationale:

- In typical business document imaging applications, software that controls the operation of the scanner and other recognition peripherals is provided. Not all scanner hardware and scan software are compatible.
- Organizations planning imaging applications should investigate and demonstrate that any product selected is capable of exporting images in a format that can be reused. Images that can not be shared are a wasted investment and could result in the loss of critical data. Therefore, avoid new deployment or migrate away from proprietary image file formats.

- TWAIN defines an open standard software protocol and Application Programming Interface (API) for communication between software applications and image acquisition devices (the source of the data). The three key elements in TWAIN are as follows:
  - The application software - An application must be modified to use TWAIN.
  - The Source Manager software - This software manages the interactions between the application and the Source. This code is provided in the TWAIN Developer's Toolkit and should be shipped for free with each TWAIN application and Source.
  - The Source software - This software controls the image acquisition device and is written by the device developer to comply with TWAIN specifications. Traditional device drivers are now included with the Source software and do not need to be shipped by applications.
- Tagged Image File Format (TIFF) is the standard format for storage and exchange of scanned images. TIFF Version 6.0 uses CCITT/ITU Group III or IV compression.

2.2.5. Use schema based eXtensible Markup Language (XML) when capturing or authoring document content that requires further automated processing by other information systems and web based clients using standard XML enabled browsers.

Rationale:

- XML is a subset of the Standard Generalized Markup Language (SGML), an ISO standard .
- XML encodes a description of a document's storage layout and logical structure with an XML Schema. It provides a mechanism to combine structured data and unstructured information content.
- XML allows information systems and applications to automatically process XML documents when the systems are combined with an XML processor.
- The XML Schema describes the required behavior of XML processors in terms of how they read XML documents, and what information they must provide to the processing application.
- The W3C established standard for XML and related technologies can be found at http://www.w3.org/TR/2004/REC-xml11-20040204/

3. Technical Topic: Electronic Mail

3.1. Practices:

3.1.1. Consider the technology and support implications when implementing security for email message transport and storage.

Rationale:

- Both private and official correspondence may require varying degrees of protection including authentication and encryption.
- Email is an inherently insecure medium. Email messages and attachments are typically transmitted as plain text and are subject to such threats as electronic eavesdropping, identity theft, invasion of privacy, spoofing, etc.

- The two basic features of email security are privacy (only the intended recipient can read the message) and non-repudiation (the recipient can be assured of the identity of the sender).
- There are currently two actively proposed methods for providing these security services: S/MIME and PGP.
- S/MIME is a version of the MIME protocol that supports encryption of messages. S/MIME is based on RSA's public-key encryption technology.
- Pretty Good Privacy (PGP) is one of the most common ways to protect messages on the Internet because it is effective, easy to use, and free. PGP is based on the public-key method, which uses two keys -- one is a public key that you disseminate to anyone from whom you want to receive a message. The other is a private key that you use to decrypt messages that you receive.
- Implementations of secure email require investments in training, infrastructure, and integration with existing email and authentication and authorization infrastructures.

3.1.2. Utilize enterprise class email services.

Rationale:

- Email should be treated as an enterprise utility.
- Providing email as an enterprise utility service removes the need for agencies to deploy redundant and possibly incompatible systems.
- Email is a strategic resource that has also become a commodity. Much like a utility service, such as electricity or phone service, appropriate resources can be directed toward developing, maintaining, and enhancing services from a statewide perspective.
- An enterprise approach to email services allows for reduced cost and increased interoperability, reliability, scalability, and accessibility.
- Critical management services such as business continuity, records management, and email hygiene can be applied from a statewide perspective.

3.1.3. Electronic mail messages are considered part of the public record and shall be managed in accordance with guidelines established by North Carolina Department of Cultural Resources (NC DCR) Office of Archives and History

Rationale:

- E-mail is a communications tool used by North Carolina government agencies.
- Electronic mail is a public record when sent or received in normal business processes (according to G.S. 121-2(8) and §132-1)
- Electronic mail may not be disposed of, erased, or destroyed without authorization from the Department of Cultural Resources.
- E-mail systems change workflow and the way government employees communicate with one another and the public. E-mail systems create records that must be identified, categorized, and appraised for specific values. Under North Carolina's Public Records Act (chapter 132 of the General Statutes of North Carolina), the e-mail content is subject to the same access and inspection conditions as other records, unless exempted from access by another statute. Privacy considerations, records retention scheduling requirements, and other laws and regulations also apply to e-mail.
- http://www.ah.dcr.state.nc.us/records/e_records/Email_8_02.pdf

3.1.4. Integrate email with applications through industry standard application programming interfaces (API).

Rationale:

- Email has become a key component of both formal and informal workflow processes. Applications can become email enabled by leveraging the statewide email service through standard APIs.
- APIs can enable applications to directly manipulate stored email messages as well as create MIME-standard outgoing messages from within an application.

3.1.5. Select email clients that integrate with the statewide email service using industry standards.

Rationale:

- The statewide email service is based on the IMAP4 and SMTP standards. A variety of email clients can seamlessly integrate with this service providing a high degree of flexibility to the end-user community.
- The statewide email service also provides web based access that is compliant with HTTP and HTTPS standards.

3.2. Standards:

3.2.1. Use Simple Mail Transport Protocol (SMTP) for sending email messages from one email server to another and from client to server.

Rationale:

- Simple Mail Transport Protocol (SMTP) is the standard transport protocol for sending electronic mail messages from one server to another. Most email systems that send messages over the internet use SMTP to send messages from one server to another.
- These email messages can then be retrieved from the server by an email client using either Post Office Protocol (POP) or Internet Message Access Protocol (IMAP).
- SMTP is also the standard protocol by which email messages are sent from an email client to an email server.
- Using Multipurpose Internet Mail Extensions (MIME) encoding, SMTP enables the transfer of text, video, multimedia, images, and audio attachments to email messages.
- SMTP is the predominate transfer protocol utilized by web browser-based email user agents.
- IETF RFC 821 establishes the standard for SMTP http://www.ietf.org/rfc/rfc0821.txt

3.2.2. Use Multi-purpose Internet Mail Extensions (MIME) to encode attachments to email messages.

Rationale:

- Multi-purpose Internet Mail Extensions (MIME), a SMTP message structure, is the standard specification for the attachment of audio, video, image, application programs, and ASCII text messages. The content type is stored in the message header as mail extensions. When the message is delivered, the player or application specific to the content type is opened so that the attachment can be viewed in its native format. If the player or application is not included with the browser, then the user

must load it. Common image and video players are included with most web browsers.

- By its definition, MIME is transformable. Although two applications may be MIME-compliant, each application can use a proprietary or custom set of extensions. The data associated with the proprietary extensions may be lost in transfer. Common protocols cut down on the risk of a loss of data occurring.
- IETF RFC 1521 establishes the standard for MIME (http://www.ietf.org/rfc/rfc1521.txt)

3.2.3. Use Internet Message Access Protocol version 4 (IMAP4) for access to email stored on the state's enterprise email services.

Rationale:

- Internet Message Access Protocol version 4 (IMAP4) is the standard protocol for access to email services. Unlike Post Office Protocol (POP3), IMAP4 provides the user the option of storing and manipulating messages on the mail server, which is important for job functions that require the user to access mail from several different clients.
- IMAP4 is also ideal for situations where the user has a low speed link to the mail server. Instead of downloading all messages to the client, IMAP4 allows the user to select which specific messages to download. If a message has several MIME attachments, the user can specify that only the text portion of the message is to be downloaded for viewing. This practice is considerably more efficient in the event that a high-speed link is not readily available.
- IETF RFC 2060 establishes the standard for IMAP4 http://www.ietf.org/rfc/rfc2060.txt

4. Technical Topic: Calendar and Scheduling

4.1. Practices:

4.1.1. Use enterprise class calendaring and scheduling services.

Rationale:

- Calendar and scheduling should be treated as an enterprise utility.
- Calendar and scheduling is intrinsically a collaboration enabler and as such is a strategic resource.
- The state provides standards-based, enterprise-class calendar and scheduling services. These services provide the state with a comprehensive, cost-effective, and scalable resource scheduling capability to all state users. Use of these statewide services removes the need for agencies to deploy redundant and potentially incompatible systems.
- An enterprise approach to calendar and scheduling services allows for increased interoperability, reliability, scalability, and accessibility.
- An enterprise approach to calendar and scheduling allows interoperability with other enterprise utility services such as directory, email, and content management.
- Adherence to open standards such as iCalendar allows multiple calendar and scheduling client to integrate with statewide services.

4.1.2. Use standard compliant calendar and scheduling client software that integrates with enterprise class calendar and scheduling services.

Rationale:

- The statewide calendar and scheduling service is based on the IETF iCalendar standards.
- Client side calendar and scheduling software (client/server or web based) that complies with the IETF iCalendar standard(s) will interoperate with the statewide calendar and scheduling service, allowing users of heterogeneous applications to schedule resources (e.g. conference rooms, parking, etc) and share calendar events.

4.2. Standards:

4.2.1. Use the iCalendar standard to exchange calendar and scheduling information.

Rationale:

- The IETF established iCalendar as a standard to represent calendar objects that can be exchanged across applications via email. iCalendar is based on the vCalendar standard, is supported by the majority of vendors as well as the statewide calendaring and scheduling service. iCalendar objects can contain single and recurring appointments as well as "to-do" list items.
- The iCalendar format is suitable as an exchange format between applications or systems. The format is defined in terms of a MIME content type. This will enable the object to be exchanged using several transports, including but not limited to SMTP, HTTP, a file system, desktop interactive protocols such as the use of a memory-based clipboard or drag/drop interactions, point-to-point asynchronous communication, wired-network transport, or some form of unwired transport such as infrared.
- IETF RFC 2445 establishes the standard for iCalendar (http://www.ietf.org/rfc/rfc2445.txt)

5. Technical Topic: Real-time Communications

5.1. Practices:

5.1.1. Implement enterprise instant messaging (EIM) and presence applications that ensure security, privacy, and compliance with records management and acceptable use policies.

Rationale:

- Real time communications capabilities such as instant messaging, presence, collaborative workspaces, etc. are being integrated in an increasing number of applications and platforms.
- Real time communications that foster collaboration can only be effective if implemented as an enterprise wide service consistent with established standards and policies.
- Real time communications can add value to personal and enterprise productivity if properly integrated into business processes, platforms, and applications.

- Public Instant Messaging (PIM) services, such as AIM, MSN, ICQ, are inappropriate for business use and are not permitted. However there may be business requirements to interoperate with PIM services. EIM gateways provide a means to integrate with Public IM services while still providing the appropriate level of security, acceptable use and regulatory compliance required for enterprise use.

5.1.2. Do not use Public Instant Messaging (PIM) services, chat websites, or chat services for real-time communications.

Rationale:

- Public Internet Messaging services include such services as AOL Instant Messenger (AIM), Yahoo Messenger, Microsoft Network Messenger (MSN), ICQ, and Jabber. These freely available services operate over the public internet.
- PIMs are inherently insecure and needlessly expose the State to a variety of threats, including:
  - Malicious code (I.e., viruses, worms, SPIM).
  - Unencrypted traffic.
  - Unattended file and application sharing.
  - Unattended desktop operating system control.
  - Exposure of confidential or private information, which could place the state in a litigious situation..
  - No record of transcripts as required by Public Records Law.
  - Inappropriate content and conduct.

5.2. Standards:

5.2.1. Use Session Initiation Protocol (SIP) as the standard for initiating real-time communications sessions in enterprise class instant messaging systems.

Rationale:

- Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. These sessions include Internet telephone calls, multimedia distribution, instant messaging, and multimedia conferences.
- SIP invitations used to create sessions carry session descriptions that allow participants to agree on a set of compatible media types. SIP makes use of elements called proxy servers to help route requests to the user's current location, authenticate and authorize users for services, implement provider call-routing policies, and provide features to users. SIP also provides a registration function that allows users to upload their current locations for use by proxy servers. SIP runs on top of several different transport protocols. SIP is used in the majority of instant messaging applications available today.
- SIP is currently on the standards track as a IETF Draft RFC: (http://www.ietf.org/rfc/rfc3261.txt?number=3261)

5.2.2. Use Session Initiation Protocol for Instant Messaging and Presence Leveraging Extensions (SIMPLE) for indicating presence in real-time communications.

Rationale:

- SIMPLE is based on the IETF signaling protocol known as the Session Initiation Protocol (SIP). SIMPLE is a set of extensions built on top of SIP that will provide for an instant messaging and presence system.
- Presence information (e.g. user availability) is increasingly being used in collaborative applications. SIMPLE is a widely supported standard for informing other users of the presence online of a user. In addition to IM, the capabilities of presence will be widely exploited in SIP-based services. As the services running on communications devices are converging, presence information can be used to manage services across different platforms. Instead of indicating presence purely in terms of a PC, presence information can apply to a number of devices and contexts, from traditional IM clients, to mobile devices, to voicemail and email, and plain telephones.
- There is an increasing trend toward extending presence to independent applications, not just human users, and enabling everything from automatic alerts and notifications to database queries via an instant messaging interface.

6. Technical Topic: Workflow

6.1. Practices:

6.1.1. Implement workflow systems that conform to the interface specifications of the Workflow Management Coalition (WfMC).

Rationale:

- As automated workflow systems continue to evolve, the complexities associated with a common approach to process definition, process repositories, object manipulation and transport, and user interfaces are enormous.
- The Workflow Management Coalition (WfMC) has established a framework for workflow standards. This framework includes five categories of interoperability and communication standards that will allow multiple workflow products to coexist and inter-operate within a network environment. This framework is contained within a Reference Model for workflow management systems that includes five interface specifications. The model includes the following:
  - Process Definition Tool.
  - Workflow Enactment Services.
  - Workflow Client Applications.
  - Invocation of Native Applications.
  - Workflow Package Interoperability
- There are many companies designing products that comply with one or more of these interface specifications. Organizations planning production workflow applications that need to route work outside of the production system for processing or decision making should work carefully with vendors and service providers to determine functional requirements and WfMC standards compliance.

- For more information about the WfMC and the work of the coalition refer to the Web site at: http://www.wfmc.org/.

6.1.2. Define and document business and workflow processes through use cases.

Rationale:

- Workflow enabled business processes need to be defined clearly, concisely, and unambiguously. Processes that cannot be described step by step cannot benefit from automation.
- Use case analysis is a method that allows for description of workflow processes from a business perspective. A use case is a narrative document that describes the sequence of events of an actor (an external agent) using a system to complete a process. Use cases provide:
- Effective communication tools guided by a structured methodology.
- Identification and consensus on business goals, participants, and outcomes of a given business process or workflow.
- Delineation of automated and manual processes required by the workflow.

6.1.3. Implement workflow technologies that enable real time monitoring of work-in-process and reporting of production statistics as well as long-term process performance metrics.

Rationale:

- Workflow technologies should support the capability to collect, analyze, and report metrics.
- Standard or customizable reports should provide detailed information about workflow artifacts, deliverables and work items for the duration of their existence.
- With process automation, identification of inefficiencies and bottlenecks should become more readily apparent. While automation can speed up processes, it can also cause too much work to be distributed to a number of people that are unable to process that work efficiently. Workflow technologies should be used to identify problems and thus provide management with the opportunity to balance and modify workflow as needed.

7. Technical Topic: Directory Services

7.1. Practices:

7.1.1. Use the statewide directory services infrastructure.

Rationale:

- Directory services should be treated as an enterprise utility.
- Using the statewide directory services has several benefits:
- The infrastructure is simplified by providing a common interface to view and manage all available resources.
- Directory services are a critical component to statewide initiatives like E-mail, identity and access management, and Electronic Commerce. The current enterprise directory is fault tolerant and highly available from any location that participates.

Time, distance, and location do not restrict access to the information contained within the services.

- Coordinated directory services will improve communication between applications, databases, and network operating systems by providing consistent, reliable information in an efficient and effective manner.
- The enterprise provides many services that are centralized in order to minimize on redundancy and increase economies of scale. Examples include time synchronization and directory replication.

7.1.2. Implement a fault tolerant solution to provide 24-hour, 7-day availability for the directory.

Rationale:

- If the directory becomes inaccessible, the resources to which a user has rights become unavailable. Therefore, a directory must be available at all times to accept authentication requests.
- This can be accomplished with a planned fail-over strategy to ensure that, if one server fails, another backup server can pick up the requests. This includes a replication strategy, with hardware solutions that include disk or system duplexing, disk or system mirroring, disk arrays, and UPSs.

7.1.3. Acquire applications and operating systems that are directory-enabled.

Rationale:

- Securing applications and their operating environments is a significant challenge. Security is a natural environment for the use of a directory. Applications can authenticate users to an external source by being directory enabled.
- The directory is better suited to provide information to the level of security necessary. Applications can be further enhanced when they are enabled to obtain an expanded set of information from the directory as appropriate. Thus, making applications more modular and consolidating administration to a central location.
- For example, an application can gather employee information from the user object in the directory. This facilitates user authentication and authorization by making the resources on that platform available to the enterprise, given when the appropriate rights are in place.

7.1.4. Use the Statewide enterprise directory as the authoritative source for directory information.

Rationale:

- Any data source is only as good as the data it contains. If that data is missing, incorrect, or incomplete, the data source cannot be depended upon as an authoritative source for that type of information.
- Directories have become much more than an authentication point for network users.
- In order to supply information on our users, network devices, and organizations, directories must be built in as complete and reliable manner as possible.
- In an enterprise directory strategy one directory must be identified as the main directory and the authoritative source for all directory information. Disparate, remote

directories and applications can synchronize with the enterprise directory to ensure reliable, current and accurate information.

7.1.5. Select applications that can externalize authentication of users to the statewide identity and access management service when making purchasing decisions.

Rationale:

- The State provides an enterprise service for the purposes of authenticating, authorizing, and managing user information.
- Give preference to vendors proposing applications that can externalize the authentication of users and determine user rights for access to the application from the enterprise directory using the established service.

7.2. Standards:

7.2.1. Use Lightweight Directory Access Protocol version 3 (LDAPv3) for directory access.

Rationale:

- LDAPv3 is the industry standard lightweight access protocol.
- LDAPv3 can provide standards based access functionality such as directories for lookups, communication mechanisms for synchronization tools, and public key retrieval.
- Commercial off-the-shelf (COTS) applications often require their own directories. Access to the application directory from outside or for the application to communicate with an external directory will require a standards based approach. When acquiring COTS applications, LDAPv3 compatibility is required.